TLP: WHITE

Advisory Alert

Alert Number: **AAA20240322** **Date:** **March 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**High**	Privilege Escalation Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34329, CVE-2023-34472)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2023-34329** - AMI MegaRAC SPx12 contains a vulnerability in BMC where a User may cause an authentication bypass by spoofing the HTTP header. A successful exploit of this vulnerability may lead to loss of confidentiality, integrity, and availability. **CVE-2023-34472**- AMI SPx contains a vulnerability in the BMC where an Attacker may cause an improper neutralization of CRLF sequences in HTTP Headers. A successful exploit of this vulnerability may lead to a loss of integrity. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Networking Z9432F-ON running on Firmware Versions prior to v3.51.5.1-18 Dell Networking S5448F-ON running on Firmware Versions prior to v3.52.5.1-10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223381/dsa-2024-148-security-update-for-dell-networking-z9432f-on-and-s5448f-on-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2022-21216)
Description	IBM has released a security update addressing a Privilege Escalation Vulnerability that exists in IntelAtom and Intel Xeon Scalable Processors which use in IBM QRadar SIEM M7 Appliances. **CVE-2022-21216**- IntelAtom and Intel Xeon Scalable Processors could allow a remote authenticated attacker to gain elevated privileges on the system, caused by an insufficient granularity of access control in out-of-band management. By sending a specially-crafted request, an attacker could exploit this vulnerability to escalate privileges. IBM recommends to apply security fixes at your earliest to protect system from potential threats.
Affected Products	IBM QRadar SIEM M7 Appliances Firmware versions before 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7144944

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.